REMARKS/ARGUMENTS

Claims 1 and 3-22 are pending in this application. Claims 1, 13 and 14 are independent. Claims 1, 3 and 13-15 are amended.

In sections 6-24 on pages 2-8, the Office Action rejects claims 1, 3, 4-8, 10-14 and 16-22 under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent No. 6,978,223 to Milliken (hereinafter "Milliken" or "R1") in view of U.S. Patent Publication No. 2002/0042837 to Ebata et al. (hereinafter "Ebata" or "R2"). The omission of claims 16 and 17 in the statement of the rejection is believed to be inadvertent. This rejection is respectfully traversed.

The problem solved by the subject matter recited in the rejected claims is how to trace a single IP packet, identified as malicious, toward its origin whilst minimizing the space requirement to store the intermediate data at each router. The claims are amended to expressly recite the role of tracing a single IP packet. The subject matter recited in the rejected claims addresses this problem by storing only one record per flow observed by a router in a given time window. This record can be seen as a canonical representation for all packets seen during a given time window. Several significant differences exist between this subject matter recited in the rejected claims and the disclosure, teaching and suggestions of Milliken (R1) and Ebata (R2).

The Office Action characterizes R1 as describing a method of tracing-back single packets. In fact, R1 describes a system for measuring network performance parameters. Thus, in R1, signature values derived from each packet received at a plurality of network nodes are used to determine one or more network performance parameters based on known network topology information. According to the subject matter recited in the rejected claims, data structures kept

by a node over configurable time windows are used to identify malicious packets, so that they can be then to traced-back to the source.

R1 describes a network equipped with a collection agent (130). The collection agent serves a plurality of nodes of interest. As recited in the rejected claims, each node maintains its repository with data structures generated and maintained in a specific way. As the information is kept locally on the routers, someone who wants to determine the path of a given malicious packet can query the closest router and trace back the packet hop by hop from the victim, which has identified the packet as malicious, toward the potential sources.

Further there is no time window in R1 as defined in step a) of the rejected claims. Rather, R1 time stamps each record calculated for each packet. As amended, the claims recite that the Time Period may be configured. Support for this subject matter can be found in the specification, for example, in paragraph [0024].

Still further, as the name says, the *FlowId* identifies a flow, and not a packet. As such, the data structures, according to the subject matter recited in the rejected claims, include one record for each flow active in the respective time window, and do not store a record for each packet as is disclosed in R1.

The foregoing differences are significant for at least the following reasons. The memory space occupied by the *FlowId* recited in the rejected claims is much smaller than the space occupied by the records in the collection agent of R1. The time needed to update the collection agent in R1 will have to be added to the processing time of each single packet forwarded by the router. Searching such a large collection of data as in R1 is more time consuming. There is no

need to transfer the *FlowIds* to any collection agent according to the subject matter recited in the rejected claim. There is such a need according to the disclosure of R1.

Even further, the Office Action cites steps 805, 505, 510, 515 with respect to the *FlowId* recited in the rejected claims. However, there is no step 805 described in R1. Rather, 805 is a node identifier used for each record stored by the collector of R1. Nevertheless, according to the subject matter recited in the rejected claims, a node identifier is unnecessary because the repository is kept at the node. Furthermore, items 505, 510 and 515 of R1 are not steps, but fields of the record 405, namely a "packet signature value," "time stamp" and "destination IP prefix." Clearly, use of these specific fields in the record 405 teaches away from the subject matter recited in the rejected claims, which pertain to a unique identifier for a flow (*FlowId*) and not in storing various parameters of a packet.

Further still, according to the disclosure, teaching and suggestion of R1, all nodes 125 of interest calculate signature values for all received packets and transmit these values to a collection agent 130. In contrast, the subject matter recited in the rejected claims prepares data structures associated with a time window (Time Period), as clearly recited in steps a) and b); the data structures store all flows collected over a time window on all interfaces at a node. This is quite different from maintaining a time-stamped record for each packet as disclosed, taught and suggested in R1. Also, there is no time window described in R1.

The *FlowId* recited in the rejected claims is calculated so as to uniquely identify a flow. R1 does not describe such a parameter at all. Rather, R1 uses, *"a hashing algorithm (e.g., MD5 message digest algorithm, secure hash algorithm .... applied to a copy of the received packet.*

Optionally, an identifier indicating the packet's destination IP prefix may be generated and appended to the packet signature value [act 915]."

R1 applies a selected function to the entire packet, since it intends to identify the packet and not the flow. The *FlowId* is calculated in a different way from the packet signature values in R1, as recited, for example, in claim 4. Further, claim 5 specifies that the *FlowId* is calculated "*applying a specified function to one or more header fields of each packet received in said flow.*"

The Office Action correctly concedes that R1 does not determine the time X of arrival of the malicious packet. In order to overcome this correctly conceded deficiency in R1, the Office Action relies on R2. See discussion of steps e and f of claim 1 in the rejection. Applicants respectfully assert that this reliance is also misplaced for at least the following reasons.

R2 describes a data transfer system and not a system for tracing-back single packets. The system of R2 includes a repeater through which streaming packets are transferred from a server (first computer) to a destination (second computer). The packets are buffered so that they arrive at the destination with a set time period (delay). Clearly, there is no point to identify the source of a malicious packet in R2, since there is just one source of the streaming packets, the server. Applicants respectfully submit that there is little resemblance between R2 and the subject matter recited in the rejected claims, included that subject matter on which R2 is relied to overcome a correctly conceded deficiency in R1.

Still further, steps e and f recited in the rejected claims define more than the difference acknowledged by the Examiner, time X. Steps e and f also recite calculating the *FlowId* for the malicious packet, identifying the *Incoming Link* by searching for the *FlowId* in all data structures

at that network node that cover the time of arrival *X*. It is respectfully submitted that R2 does not disclose, teach or suggest this subject matter. Further, R1 does not describe data structures associated with time windows. Neither R1 nor R2 describe searching only the data structures pertinent to time X.

Paragraph [015] of R2 describes the repeater, which is a stand-alone network element and not a system provided at a network node as recited in the rejected claims. None of the elements of the repeater (the packet memory, the packet analyzer, the header analyzer, the packet manager, and the packet sending controller) described in this paragraph constitute a disclosure, teaching or suggestion of subject matter recited in the rejected claims.

While the repeater is provided with a flow registration table 104, this table contains information is related to each streaming flow, as shown in FIG. 4. The information stored in this table is different than the information stored in the data structures recited in the rejected claims since R2 uses the table to determine the destination address (output port on the repeater) of the packets.

Paragraph [0049] of R2 describes that the packet analyzer 101 searches the flow registration table 104 for the flow identifying information of a received packet to determine whether the received packet is a streaming packet of a flow registered in the flow registration table 104. However, this text does not disclose, teach or suggest the subject matter recited in the rejected claims in steps e and/or f (determining the time of arrival *X* of the malicious packet at the network node, computing *FlowId* for the malicious packet, identifying the *Incoming Link* for

the malicious packet by searching for the *FlowId* only in data structures at that network node that cover the time of arrival *X*).

Paragraph [0056] of R2 says that the packet manager 105 registers the address, port number, time stamp, and the sequential number for each flow identified by a pair of address and port number, into the flow registration table 104, as in Figure 5. The subject matter recited in the rejected claims does not pertain to storing time X into the data structures. In the rejected claims, time X is used to select which data structures maintained at the respective node should be searched for *FlowId* of the packet.

Claims 3-8 and 10-12 are allowable based at least on their dependence from claim 1 for the reasons stated above in connection with claim 1.

Claims 13 and 14, from which claims 16-22 depend, contain several recitations similar to the recitations in claim 1 cited above in connection with the argument traversing the rejection of claim 1. Thus, to the extent that claims 13, 14 and 16-22 contain recitations similar to the recitations in claim 1 argued above, claims 13, 14 and 16-22 are allowable for at least the same reasons as claim 1.

Further regarding claims 13, 14 and 16-22, the claims define a mode of operation different than that recited in claim 1 because *FlowId* is calculated using data provided by a flow management system according to the subject matter recited in claims 13, 14 and 16-22. Accordingly, the subject matter recited in claims 13, 14 and 16-22 takes advantage of the use of a flow management system in a modern router. None of the disclosure in Miliken and Ebata pertains to such a system.

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 1, 3-8, 10-14 and 16-22 as allegedly being unpatentable over Milliken in view of Ebata be withdrawn.

In sections 25-27 on pages 8-9, the Office Action rejects claims 9 and 15 under 35 U.S.C. §103(a) as allegedly being unpatentable over Milliken in view of Ebata and further in view of "Hash Based IP Traceback" by Snoeren et al. (hereinafter "Snoeren"). This rejection is respectfully traversed.

Claims 9 and 15 are allowable based at least on their dependence from claims 1 and 14, respectively, for at least the reasons stated above in connection with the rejection of claims 1 and 14. Snoeren fails to overcome the deficiencies in Milliken and Ebata described above in connection with the rejection of claims 1 and 14.

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 9 and 15 as allegedly being unpatentable over Milliken in view of Ebata and further in view of Snoeren be withdrawn.

CONCLUSION

While we believe that the instant amendment places the application in condition for allowance, should the Examiner have any further comments or suggestions, it is respectfully requested that the Examiner telephone the undersigned attorney in order to expeditiously resolve any outstanding issues.

RECEIVED
CENTRAL FAX CENTER
SEP 05 2007

Application No: 10/730,926
Attorney's Docket No: ALC 3106

In the event that the fees submitted prove to be insufficient in connection with the filing of this paper, please charge our Deposit Account Number 50-0578 and please credit any excess fees to such Deposit Account.

Respectfully submitted,
KRAMER & AMADO, P.C.

Date: September 5, 2007

Terry W. Kramer
Registration No.: 41,541

KRAMER & AMADO, P.C.
1725 Duke Street, Suite 240
Alexandria, VA 22314
Phone: 703-519-9801
Fax: 703-519-9802